In the claims

1. (previously presented) A method of transporting a document comprising:

encrypting an original document;

transmitting an image of the original document to a system of ~~the~~ a recipient;

assuring that the system of the recipient has received transmission of the image of the original document;

destroying the original document at a system of a sender after transmitting the image of the original document to the system of recipient, where the original document is destroyed at the system of the sender only after the system of the sender has received assurance that the system of the recipient has received transmission of the image of the original document;

decrypting the image of the original document;

printing a copy of the image of the original document at the system of the recipient; and

certifying that the copy of the image of the original document was received from a sender, by at least a public notary notarizing the copy of the image of the original document as has been printed.

2. (original) The method of claim 1 further comprising assuring that the system of the recipient is enabled to receive a transmission.

3. (cancelled)

4. (previously presented) The method of claim 1 further comprising placing the received transmission in a storage device of the system of the recipient, wherein the public key of the sender is used by the recipient to access the image of the original document in the storage device.

5. (original) The method of claim 1 further comprising adding a global universal identification to the encrypted original document.

6. (original) The method of claim 5 wherein the global universal identification includes a time component and a unique machine identifier.

7. (original) The method of claim 6 wherein the unique machine identifier is a machine address code (MAC).

8. (original) The method of claim 1 further comprising notarizing the original document.

9. (cancelled)

10. (original) The method of claim 1 wherein encrypting an original document further comprises use of a private key of the sender.

11. (original) The method of claim 10 wherein encrypting an original document further comprises use of a public key of a recipient.

12.-18. (cancelled)

19. (currently amended) An imaging apparatus comprising:

a processor;

a storage device; and

software operable on the processor to:

encrypt an original document;

transmit a copy of the original document to a recipient, a system of the recipient assuring that the system of the recipient has received transmission of the copy of the original document; and

destroy the original document after transmitting the copy of the original document to recipient,

wherein the original document is destroyed at the imaging apparatus only after the imaging apparatus has been assured that the recipient has received the copy of the original document.

20. (original) The imaging apparatus of claim 19 wherein the software is further operable on the processor to decrypt the image of a copy of an original document using a public key of a person sending the document.

21. (original) The imaging apparatus of claim 19 wherein the storage device stores an image of the original, transmitted document until an indication that the transmitted document is received.

22. (original) The imaging apparatus of claim 19 wherein the software is further operable on the processor to poll an other imaging apparatus to which the image of the original document is transmitted to determine if the other imaging device is enabled to receive the transmission of the original document.

23.-32. (cancelled)

33. (currently amended) A computer-readable medium having a program available thereon for causing a suitably programmed information-handling system to transport documents between a first imaging device and a second imaging device by performing the following when such program is executed on the information-handling system:

encrypting an original document;

transmitting the original document from the first imaging device to the second imaging device, such that the second imaging device receives an image of the original document, wherein the second imaging device is under control of the recipient;

transmitting an acknowledgment of receipt of the image of the original document from the second imaging device, such that the second imaging device assures that the second imaging device has received transmission of the image of the original document; and

destroying the original document at the first imaging device in response to receiving the acknowledgment from the second imaging device, such that the original document is destroyed at the first imaging device only after the first imaging device has been assured that the second imaging device has received the image of the original document,

wherein the computer-readable medium comprises a storage device.

34. (original) The computer-readable medium of claim 33 having a program further capable of performing the following when such program is executed on the information-handling system:

decrypting the image of a copy of an original document using a public key of a person sending the document; and

printing a copy of the image original document at the system of the recipient.

35. (currently amended) An apparatus for transporting a document comprising:

a storage device;

means, implemented at least in the storage device, for encrypting an original document;

means, implemented at least in the storage device, for transmitting an image of the original document to a system of the recipient;

means, implemented at least in the storage device, for destroying the original document at the apparatus after transmitting the original document to the system of the recipient, such that the

system of the recipient assures that the system of the recipient has received transmission of the image of the original document, and such that the original document is destroyed at the apparatus only after the apparatus has been assured that the image of the original document has been received by the system of the recipient;

means, implemented at least in the storage device, for decrypting the image of the original document; and

means, implemented at least in the storage device, for printing a copy of the image original document at the system of the recipient.

36. (original) The apparatus of claim 35 further comprising means for assuring that the system of the recipient is enabled to receive a transmission.

37. (original) The apparatus of claim 35 further comprising means for assuring that the computing device of the recipient received the transmission before destroying the original document.

38. (original) The apparatus of claim 35 further comprising means for certifying that the copy of the image was received from a sender.

39. (original) The apparatus of claim 35 further comprising means for identifying the encrypted original document.